

Is medhaint.com a scam? TrustSniffer's high-risk assessment: 0/100

medhaint.com

Verdict

0

OUT OF 100

CRITICAL RISK

medhaint.com shows high-risk / scam indicators.

This assessment found strong scam indicators. Do not pay, sign in, or share personal details with this site.

Sensitive Interaction Risk

Governance Risk

Assessed 2026-08-20 by automated analysis. Classification confidence 55%.

What this site appears to be

Simple landing page for 'Medha Int' focused on wellness messaging; contains cookie consent and a brief promotional line about an AI builder. No contact details, commerce, login, or financial flows visible.

Evidence status and limitations

- Evidence completeness: UNKNOWN
- The real-world operator identity was not independently verified.
 - Module-level completeness metadata is unavailable for this legacy report.

At a glance

The checks that decide most of this verdict.

Malware engines	4 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	26% confidence AbuseIPDB, 13 reports; shared hosting inflates reports	CLEAR
Domain age	22 years old Registered history	CLEAR
Web archive	Archived since 2013 Public history exists	CLEAR
Certificate	Encrypted connection Issued by GoDaddy TLS Intermediate CA DV - R1v1	NOTED

The page as captured

https://medhaint.com/

 GoDaddy Airo Try Airo AI Builder | [Start for free](#)



What medhaint.com served when TrustSniffer captured it on 2026-08-20. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: more than 10 years (registration continuity).
- Public web-archive history exists since 2013.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

Kaspersky flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

Medha Int is a minimal informational landing website presenting “Empowering Your Wellness Journey” alongside promotional messaging for the Airo AI Builder, including a free-credit offer and a “Start for free” prompt; its apparent purpose is brand or informational engagement rather than visible commerce or financial services.

Scam/Impersonation Risk

Confirmed external threat detections and blacklist status create a critical security concern despite the absence of visible login forms, payment flows, wallet functions, or explicit impersonation indicators on the homepage. The available evidence does not establish that the site itself operates the reported infrastructure issues: abuse reports concern a shared Amazon content-delivery IP, but the domain-level blacklist and malicious detections remain material contradictions. The homepage’s limited content and absence of a clear operational identity also provide little context for resolving those warnings. No identity contradiction or page-level brand impersonation was observed. The site’s published contact presentation includes the address `info@example.come`, an

address-format anomaly that may reflect a deliverability-breaking typo or possible typosquat and should be treated as a contact-channel integrity concern.

EVIDENCE

- External reputation checks recorded 4 malicious and 1 suspicious detections for the domain, with confirmed blacklist status.
- The homepage runtime generated 18 external XHR requests, including 15 non-whitelisted requests, and 2 non-whitelisted POST requests; no hidden forms or password-submission forms were detected.
- The site's homepage was classified as an informational landing page with no visible login, commerce, financial, or wallet-connect flow.

Regulatory Verification Notes

The site presents itself as “Medha Int” and displays a copyright notice for 2025, but the available pages do not independently verify the real-world operator. No regulated financial activity is visible, and no licensing claim or license number is presented; this is a transparency point if the site later solicits regulated services, investment, or financial transactions, not standalone evidence of fraud. Domain registration is long-established and uses GoDaddy, while registration privacy means the published registrant details do not independently connect the domain to the apparent organization. The available broker-context dataset did not produce a match, but that is limited reputational context rather than a regulatory determination.

EVIDENCE

- Domain registered 2005-01-23 and recorded as 21.58 years old; registrar: GoDaddy.com, LLC.
- Served from AS16509, Amazon.com, Inc., US.
- TLS certificate: GoDaddy TLS Intermediate CA DV - R1v1, Domain Validation (DV), valid to 2026-11-01T15:20:10+00:00.
- The homepage displays “Medha Int,” “Contact Us,” and “Copyright © 2025 Medha Int - All Rights Reserved,” without a visible legal-entity or licensing disclosure.

What to Verify Next

Before any sensitive interaction, the apparent operator should be independently confirmed through an offline or otherwise trusted channel, rather than relying solely on the website's own branding. If the site later requests credentials, payment, financial deposits, or regulated-service participation, the relevant legal entity and any claimed authorization should be checked directly against the applicable official registry, and payment protections should be used only after that verification. Official support and contact channels should also be confirmed independently.

EVIDENCE

- The homepage contains no visible sensitive form, login mechanism, payment function, or financial workflow that would support safe validation through an account transaction.
- The site's operator identity is not independently verified by the available evidence.
- External reputation warnings remain unresolved and warrant confirmation before any transition from passive viewing to sensitive activity.

Summary Verdict

The overall posture is critical, with a material risk of harmful consequences from sensitive interaction. The website may appear to be a simple wellness landing page, but that presentation does not overcome the confirmed external contradictions or establish a trustworthy operator identity.

Infrastructure Integrity

The website is protected by a CDN/WAF layer using Amazon edge infrastructure; observed addresses belong to edge servers, and no origin candidate was identified. This reduces direct exposure of the origin environment but is only a mitigating infrastructure characteristic and does not validate the website's legitimacy.

Closing Assessment

Prospective users should restrict activity to passive viewing and should not submit credentials or conduct financial interactions unless independent operator and authorization checks first resolve the outstanding security concerns.

Written analysis generated 2026-08-20 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

2 findings contributed to this verdict, raised by registration and ownership, analysis engine, behaviour in a sandbox, external reputation.

01 Governance Risk

- The registration record withholds contact details for the operator.
Registration and ownership rule:KF_WHOIS_HIDDEN
- Registration details are held behind a privacy service, so no operator is named publicly. This is common and legal, and it also means there is nobody to check.
Registration and ownership rule:KF_WHOIS_PRIVATE

02 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.
Analysis engine signal:direct_threat
- The page made background requests to destinations TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_XHR
- Most of what the page loaded came from other domains rather than from this one.
Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_HIGH
- The page sent data to a destination TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS
- The page exchanged network traffic with destinations TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_TRAFFIC
- An external threat feed lists this domain: either Google Safe Browsing marked it malicious, or a significant number of malware engines flagged it.
External reputation rule:EXT_BLACKLIST_CRITICAL

Signals weighed against the site

- AbuseIPDB: 13 reports on hosting IP 76.223.105.230 (Amazon.com, Inc., Content Delivery Network), 26% confidence. The reports are attributed to shared infrastructure, not specifically to this website.

Identity verification

Status	UNVERIFIED
Identity score	30/100
Identity verification confidence	25%

- No on-site identity signals detected

Identity verification measures whether the site can be independently connected to a real-world brand or person. It is separate from the classification confidence.

What TrustSniffer observed

First-party facts recorded during the assessment of medhaint.com.

- The request stayed on medhaint.com. It was not redirected to another domain. CLEAR
- Registration is published under GoDaddy.com, LLC. CLEAR
- DNS for this domain is served by domaincontrol.com, across 2 name servers. NOTED
- The registration is paid up to 2029-01-23. CLEAR
- The earliest public archive of this site is from 2013-06-13. CLEAR
- It is hosted on AMAZON-02, from a server in US. NOTED

Domain intelligence

Registrar	GoDaddy.com, LLC
Hosting	AMAZON-02 - Amazon.com, Inc., US
Country	US
Server IP	76.223.105.230
Name servers	NS51.DOMAINCONTROL.COM, NS52.DOMAINCONTROL.COM
SSL issuer	GoDaddy TLS Intermediate CA DV - R1v1
SSL expiry	2026-11-01
Domain age	21.58 years (continuous registration)
Domain expiry	2029-01-23
Archive first seen	2013-06-13
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 4 flagged AbuseIPDB: 26% confidence, 13 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about medhaint.com at assessment time. It is a starting point for your own judgement, not a guarantee: a high score means the signals were consistent with a legitimately operated site, a low or critical score means several risk patterns were present.

TrustSniffer assesses a website from the evidence it can collect at a point in time: domain registration and age, hosting and certificate, the content the site served, and third-party reputation feeds. A score is a summary of that evidence, not a guarantee and not a legal finding. There is no human rating and no user review in it. A site can change after it is assessed.

This report online: <https://trustsniffer.com/report/medhaint.com> · assessed 2026-08-20